HPE OpenNFV Partner Program VNF Testing—FusionLayer

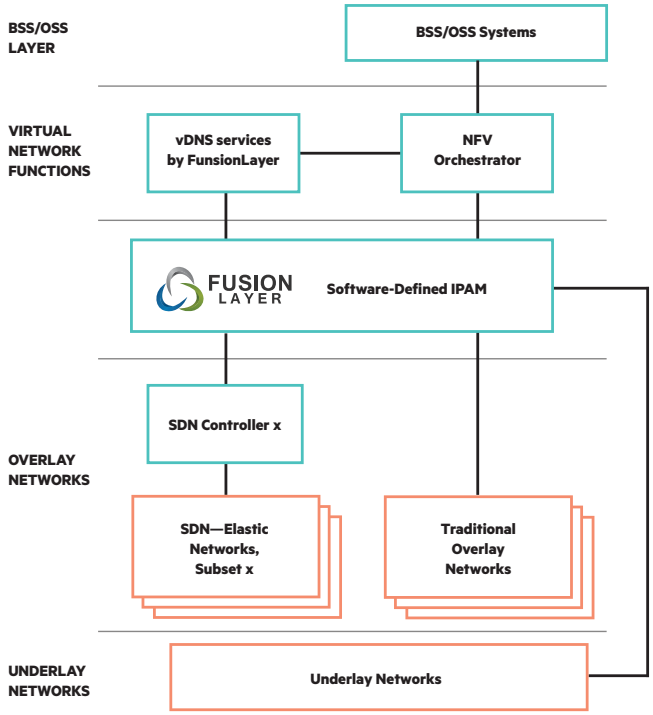

Figure 1: Reference Architecture

HPE OpenNFV Partner Program

With the right network functions virtualization (NFV) platform, communication service providers (CSPs) enjoy the freedom to build a custom end-to-end solution based on individual IT and customer needs. This approach facilitates collaboration with third parties based on open standards, regardless of vendor. The HPE OpenNFV Partner Program supports this degree of flexibility and openness by including emerging independent software vendors (ISVs) along with leading network equipment providers (NEPs), technology vendors, and service providers. The result: CSPs can transition to NFV in a way that best suits the business and IT.

The HPE OpenNFV Partner Program includes

Technology partners—Top-performing technology companies and vendors that collaborate on technology innovation, integration, and support.

Application partners—ISVs are self-tested in a remote OpenNFV virtual environment (referred to as "OpenNFV tested"), are joint-tested in physical HPE labs (referred to as "OpenNFV ready").

Services partners—Systems integrators

Testing in the OpenNFV Labs

OpenNFV Labs provides a one-stop center where integration, collaboration, and testing occur in a safe environment ahead of deployment to carrier networks. With OpenNFV Labs, CSPs gain access to software development kits (SDKs), application program interfaces (APIs), training, and integration resources to get applications tested and ready for CSPs, advancing innovation while reducing risks. There are currently five HPE OpenNFV Labs locations: Fort Collins, CO; Houston, TX; Grenoble, France; Tel Aviv, Israel; and Seoul, South Korea.

Partner solutions are tested in the OpenNFV labs leveraging our reference architecture and NFV System. The NFV Reference Architecture supplements existing systems by identifying the HPE products that readily integrate with scalable, high-performing, and robust NFV solutions. NFV System offers a fully integrated, turnkey solution.

The labs validate partner solutions in three tiers—silver, gold and platinum—which tests onboarding and basic functionality, performance and scalability, and continued functionality through software updates and changes.

Partner Introduction

FusionLayer specializes in software-defined IP Address Management (IPAM) and virtualizable DNS solutions designed to simplify your networked world. Based on patented technologies that provide x10 performance advantage over competing solutions, FusionLayer furnishes CSPs with unified network visibility and API-based provisioning capability for all network-related resources. Through industry partnerships, 9 out of the world's 10 largest service providers leverage FusionLayer.

To learn more, visit **fusionlayer.com**.

Partner Solution Overview

Many CSPs continue to manage their network blocks, prefixes and subnets using static spreadsheets or traditional IP Address Management (IPAM) solutions. While feasible in monolithic network environments that utilize manual management processes, the traditional tools cannot be properly integrated with the automated workflows at the core of Network Function Virtualization (NFV) and Software-Defined Networking (SDN).

Furthermore, to avoid overlap and the resulting service outages while making the transition from the traditional networking model into the new era, it is paramount that the entire IP inventory is managed and provisioned using a single authoritative solution.

FusionLayer Infinity is a software-defined IP Address Management (IPAM) solution that enables unified management of all network resources such as blocks, networks and individual IP addresses within a single solution. With built-in connectors that enable seamless integration with OpenStack, it provides CSPs with real-time visibility into network blocks consisting of both traditional and NFV-enabled networks.

To simplify adherence to NFV best practices, FusionLayer also automates the generation of Unique Identifiers (UIDs) used in connection with Virtual Network Function (VNF) elements. Once a new UID has been created based on a predefined pattern, it is automatically appended to a network-specific default zone and pushed into the secure FusionLayer vDNS service.

Solution Benefits

FusionLayer Infinity

- Unified real-time visibility into all network blocks and subnets
- Facilitates multitenant use-cases by supporting network overlap and delegated management
- "Network CMDB" functionality with configurable data structure with REST access (read, write, remove)
- REST-based provisioning of network prefixes, IP addresses, UIDs, names and network attributes
- Object-oriented architecture with mapping support—NAT, IPv4—IPv6, VRF, VLAN—VXLAN, etc.
- Native integration with OpenStack via Neutron API and/or IPAM driver
- Supports centralized management of integrated DNS and DHCP services
- Plug-and-play integration with various third-party orchestrators and SDNs

FusionLayer DNS

- High-performing virtualizable DNS server with hardened OS and embedded SQL backend
- Built-in security with firewall, intrusion prevention, rate-limiting and Response Policy Zones (RPZ)
- Supports advanced query logging, syslogging and SNMP trapping
- Service performance can be scaled vertically (adding CPU) or horizontally (multiple instances behind VIP)
- Supports centralized management and DNS change provisioning via FusionLayer Infinity

Application Functionality within OpenNFV Reference Architecture

FusionLayer Infinity

- Provides the ability to manage all network blocks and subnets centrally within a single unified system
- Automatically pulls network changes from OpenStack into software-defined IPAM (via Neutron API)
- Automates UID-generation based on network-specific patterns and default zones, with change provisioning to DNS
- Supports centralized management of integrated vDNS (and vDHCP) services
- Provisions unused prefixes and IP addresses to third-party orchestrators via REST

FusionLayer DNS

- Provides a vDNS service as a Virtualized Network Function (VNF)
- Provides recursion and/or serves out authoritative requests for UID zones
- Protects the OpenNFV architecture through "DNS Firewall" set-up

Testing Statement

To facilitate the transition from traditional networking models into agile networking through next-generation technologies such as NFV and SDN, CSPs need a centralized management and provisioning system that is authoritative for all network-related information and/or resources. In the absence of such a system, it becomes difficult if not impossible to create fully automated workflows that maximize the ROI of the NFV investment.

Equally important, the lack of such a unified system often leads to overlap and/or the use of duplicate IP addresses, which in production environment could cause severe service disruptions.

To address the business problems outlined above, FusionLayer has deployed a Proof-of-Concept environment in HPE's NFV testing laboratory consisting of one FusionLayer Infinity and one FusionLayer DNS server instance. The purpose of the POC was to validate the interoperability between FusionLayer products and HPE's NFV-I platform, and to confirm the functional benefits outlined elsewhere in this document.

Upon a successful completion of the POC, we believe that CSPs that deploy both HPE NFV-I and FusionLayer solutions will be in the position to achieve the following business benefits:

- Improve the ROI on their NFV investment through the elimination of unnecessary manual steps
- Avoid service disruptions caused by unintended network overlap and/or duplicate IP address assignments
- Implement the NFV best practice of using UIDs as opposed to traditional names

Testing Details and Proof Points

The POC environment consisted of two Virtualized Network Function Component (VNFC) instances. These corresponded to two Virtualized Network Function (VNF) instances. The equipage of the individual VNFC instances were the following:

- VNFC-1: FusionLayer Infinity 2.2.1.0—software-defined IPAM server instance
- VNFC-2: FusionLayer DNS 3.0-2—DNS software appliance running as a vDNS server instance

The initial VNFC images were taken from a FusionLayer lab setup running 64b CentOS guest operating system under VMware and ported/deployed to the HPE Helion OpenStack NFVI running the same under KVM. The CentOS operating system was automatically hardened during the installation of the initial VNFC image.

During testing, communications between the VNFC instances were carried out over a public network.

Once the VNFCs images were installed, FusionLayer Infinity was configured as the hidden primary for the DNS set-up and the following test sets were carried out:

Test Set 1: Validate the basic functionality of FusionLayer Infinity and FusionLayer DNS on HPE NFVI platform.

Result 1: It was verified that both FusionLayer server instances were running on NFVI platform as designed.

Test Set 2: Validate the import and management of existing network blocks into FusionLayer Infinity

Result 2: An existing CSV file containing three existing Class B and 100 Class C networks were successfully migrated into FusionLayer Infinity. One Class C network simulating a data center network was integrated with a remote DHCP server and verified to function as intended.

Test Set 3: Validate the integration between OpenStack (via Neutron API) and FusionLayer Infinity

Result 3: Integrated FusionLayer Infinity with a remote OpenStack server using the Neutron API for integration. Verified that networks in OpenStack were read into FusionLayer Infinity and the changes effected by OpenStack were reflected in the networks visible in FusionLayer Infinity.

Test Set 4: Validate the primary—authoritative secondary integration model set up between the two instances.

Result 4: It was verified that FusionLayer Infinity was successfully managing the master zones files for which FusionLayer DNS was configured as the authoritative DNS secondary. Also verified that general DNS protocols such as NOTIFY and IXFR functioned as intended.

Test Set 5: Validate the REST-based assignment of UIDs and provisioning into production DNS

Result 5: It was verified that the REST API could be queried for UIDs for a specific network; that the UID was successfully assigned to the requesting client and appended to the default zone set for the network in questions; and that the UID was pushed into the authoritative DNS service and served out.

Based on the above results, we concluded that the FusionLayer concept was running well on HPE NFVI platform, and that the functionality described in this document worked as intended. To ensure the continuity of the shared solution described herein, the test environment was being run continuously for approximately two weeks.

Solution Benefits

Communication Service Providers can leverage the pre-tested and integrated solutions from partners such as FusionLayer within the NFV ecosystem, significantly reducing solution selection and deployment times. CSPs can also see the details of the tests performed, testing methodology and the automation involved, along with the results of the tests.

Conclusion

Based on the validation testing carried out by FusionLayer in HPE's NFV test laboratory, we were satisfied that the general architecture and the solution benefits outlined in this document have been accurately described. We therefore concluded that the business benefits outlined in this document are also attainable, and will be happy to repeat the same during new POCs repeated onsite at interested CSPs.

HPE Contact Information

Jeff Kibodeaux
Partner Program Manager
opennfvpartners@hpe.com

FusionLayer Contact Information

Laurent Werner
Solution Consultant
cloud@fusionlayer.com

Learn more at
hpe.com/csp/nfv
or by following @hpe_nfv

Sign up for updates

4AA6-6464ENW, July 2016